LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, NOVEMBER 20, 2020

PERSPECTIVE

CPRA's impact on CCPA enforcement and compliance

By Sheri Porath Rockwell and Alexis Miller Buese

California is once again on the forefront of data privacy law with the passage of Proposition 24, the California Privacy Rights Act. The law amends 2018's California Consumer Privacy Act by creating the nation's first data privacy enforcement agency and expanding consumers' rights with respect to their personal information. The initiative also increases litigation and enforcement risks by, among other things, creating an agency dedicated to enforcement of the law, expanding the categories of personal information subject to suit in the event of a data breach or exfiltration of data, and by removing the 30-day notice to cure for administrative enforcement actions.

Most of the CPRA's provisions go into effect on Jan. 1, 2023, with a lookback to January 2022, giving covered business valuable time to prepare. This article highlights some of the more significant features of the CPRA that are likely to impact consumers and businesses alike.

Opt-Out Rights for Behavioral Advertising

The CPRA gives California residents the ability to stop a business from sharing their personal information for the purpose of engaging in "cross-context behavioral advertising" — ad targeting based on tracking individuals' activity across different websites or applications, or their interaction with other businesses.

What makes this provision powerful is that, by January 2023, consumers will likely be able to exercise opt-out choices across millions of websites and apps at once, using global privacy tools already in development. Today's cumbersome site-by-site opt-out process will be replaced by universal opt-out signals that businesses subject to the CCPA will be required to recognize.

Automated Decision-Making: Access and Opt-Out Rights

The CPRA also creates opt-out rights with respect to businesses' use of "automated decision-making technology," which includes profiling consumers based on their "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." California consumers will be able to prevent businesses from using their personal information for such profiling, even if it is done in-house and not shared with any third parties. In addition, the CPRA requires profiling transparency, as consumers can also demand the disclosure of "meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."

Sensitive Information: New Disclosure Obligations and Opt-Out Rights

The CPRA creates a new category of information, "sensitive personal information," which includes certain government-issued identifications (such as social security, driver's license, or passport numbers), account login information, mail and email contents, or data pertaining to precise geolocation, racial origin and other information about protected classes. Additionally, consumers can opt out of the use of sensitive information collected by a business for the purpose of inferring characteristics about consumers.

Audits and Privacy Risk Assessments

Businesses that regulators determine pose a "significant risk" to consumers' privacy (based on their size and the nature of their data processing activities) will be required to perform annual cybersecurity audits and perform "regular" risk assessments with respect to their processing of personal information, which will incorporate a cost-benefit analysis that weighs the potential risks to consumers' privacy rights against the benefits of processing to the business, stakeholders and consumers.

Changes to the Private Right of Action

The CPRA authorizes an expansion of the private right of action by adding email addresses and passwords or security questions to the list of personal information categories that, if subject to a data breach, may give rise to a private right of action. Because emails and passwords are often impacted in data security incidents, adding this category of personal information is likely to increase litigation risk for businesses subject to the CCPA.

CPRA also creates uncertainty with respect to the private right of action, specifically the cure provisions. Currently, the CCPA authorizes private citizens to bring suit for statutory damages if a breach was caused by a business's failure to implement reasonable security measures, and the business is given a 30-day notice to cure. Because the cause of action must be based on an alleged breach of the duty to maintain reasonable security measures, a "cure" could likely include steps to fortify security measures. The CPRA, however, appears to foreclose this option, as it states, "the implementation and maintenance of reasonable security procedures and practices" does not constitute a cure with respect to [a] breach." Unless this provision is clarified, courts will likely be called up on to decide what does or does not constitute a cure under the

CCPA's private right of action.

Expanded Enforcement and Removing Mandatory Opportunity to Cure

The new Privacy Protection Agency created by the CPRA will be the first of its kind in the United States, with the power to issue regulations and, along with the attorney general, enforce the law. The agency will also oversee audits, educate California consumers about their privacy rights, and act as a liaison to the legislature and other agencies.

Businesses subject to enforcement actions by the agency or the attorney general will not have the benefit of a mandatory 30-day notice to cure under the CPRA.

The Privacy Protection Agency has broad investigatory powers and is authorized to bring enforcement actions in accordance with California's Administrative Procedure Act. Specifically, violations can only be determined after a noticed administrative hearing. If, through the hearing process, the agency determines a violation or violations have occurred, it may issue a cease and desist order and/or issue an administrative fine between $2,500 and $7,500 per violation, and must state the reasons for doing so in writing.

Key Takeaways

The CPRA creates a host of new obligations for businesses, only a few of which are highlighted here. Covered business should carefully review the nuances brought by the CPRA, and consider how their existing data governance programs need to be updated. Business should also think about determining how to allocate budget dollars to build out compliance capabilities and consider adjustments to digital advertising strategies. And, while implementing changes to the privacy compliance programs, covered business must still fulfill their obligations under the current version of the CCPA. ■

This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer- client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect the views of the firm.

Sheri Porath Rockwell *is an associate in Sidley Austin's Century City office and a member of the firm's CCPA Litigation Task Force. Her practice focuses on privacy and cybersecurity law, as well as complex commercial litigation. She can be reached at sheri.rockwell@sidley.com.*

Alexis Miller Buese *is a partner in the Century City office of Sidley Austin LLP. Alexis handles all aspects commercial litigation, including consumer class action litigation, and she is a member of the firm's CCPA Litigation Task Force. She can be reached at alexis.buese@sidley.com.*